UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,375	11/19/2003	Peter Szor	SYMC1040	9545

34350 7590 06/20/2007

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
06/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/718,375	SZOR ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *30-33* is/are allowed.

6)☒ Claim(s) *1-10,13,24-26 and 28* is/are rejected.

7)☒ Claim(s) *11,12,14-23,27 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070612*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 23 May 2005.

2. Claims 1-33 are pending for examination.

3. Claims 1-10, 13, 24-26 and 28 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-10, 13, 24-26 and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Muttik et al, U.S. Patent Application Publication 2003/0023864 A1.

5. As per claim 1; "A method comprising:

stalling a file system event,

said file system event including a file name [ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan (i.e., malware/viral) request receiving/processing/result servicing (stalling file system event(s), inclusive of Windows/Unix, etc., type file systems with directory/file naming/file name extension architectures, while malware detection/processing performed), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

parsing said file name to obtain at least

a last file name extension of said file name [ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), inclusive of Windows/Unix, etc., type file systems with directory/file naming/file name extension architectures, with file name extension parsing as a filtering parameter or complexity metric for the malware detection/processing), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

determining whether said last file name extension is

the only file name extension of said file name [ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing inherently determining if the at least one file name extension is the only file name extension), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

upon a determination that said last file name extension is

not the only file name extension of said file name,

determining whether said last file name extension is

a dangerous file name extension [ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing inherently determining if the at least one file name extension is the only file name

extension, such that for the case of not having determined that a second file name extension exists, the test is moot), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

upon a determination that said last file name extension is

a dangerous file name extension,

generating a notification [ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing inherently determining if the at least one file name extension is the only file name extension, and upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

As per claim 24, this claim is the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A system comprising:

an anti-viral application, said anti-viral application for

intercepting and

stalling

a file system event including a file name; and

a detection application communicatively coupled to

said anti-viral application, said detection application for

detecting a dangerous file name extension present in said file name.".

6. Claim 2 ***additionally recites*** the limitation that; "The method of Claim 1, further comprising:

implementing protective actions.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation (i.e., protective actions)/annunciation processing is performed), as broadly interpreted by the examiner.).

7. Claim 3 ***additionally recites*** the limitation that; "The method of Claim 1, further comprising:

terminating said file system event.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation (i.e., terminating said file system event)/annunciation processing is performed), as broadly interpreted by the examiner.).

8. Claim 4 ***additionally recites*** the limitation that; "The method of Claim 1, further comprising:

intercepting said file system event.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (intercepting said file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), as broadly interpreted by the examiner.).

As per claim 26, this claim is the system claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; "The system of Claim 24, wherein

said anti-viral application comprises:

an intercept module

for intercepting and

stalling

said file system event including said file name.".

9. Claim 5 ***additionally recites*** the limitation that; "The method of Claim 4, wherein said file system event originates from

a selected category of applications.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (intercepting said file system event(s), such as e-mail, word processing, network object/communications processing 'selected category of applications', with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), as broadly interpreted by the examiner.).

10. Claim 6 ***additionally recites*** the limitation that; "The method of Claim 5, wherein said selected category of applications is

a network application.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (intercepting said file system event(s), such as e-mail, word processing, network object/communications processing 'selected category of applications', with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), as broadly interpreted by the examiner.).

11. Claim 7 ***additionally recites*** the limitation that; "The method of Claim 4, wherein said file system event originates from

an instant messaging application.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (intercepting said file system event(s), such as e-mail (i.e., instant messaging being real time e-mail), word processing, network object/communications processing 'selected category of applications', with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), as broadly interpreted by the examiner.).

12. Claim 8 ***additionally recites*** the limitation that; "The method of Claim 4, wherein said file system event originates from

an electronic mail (e-mail) application.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (intercepting said file system event(s), such as e-mail, word processing, network object/communications processing 'selected category of applications', with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation/annunciation processing is performed), as broadly interpreted by the examiner.).

13. Claim 9 ***additionally recites*** the limitation that; "The method of Claim 4, wherein said file system event originates from

a peer-to-peer (P2P) network application.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), inclusive of Windows (i.e., so configured as a standard peer-to-peer (P2P) network)/Unix, etc., type file systems with directory/file naming/file name extension architectures), as broadly interpreted by the examiner.).

14. Claim 10 ***additionally recites*** the limitation that; "The method of Claim 1, further comprising:

obtaining said file name from

said file system event.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), inclusive of Windows (i.e., inclusive of the associated obtained file names)/Unix, etc., type file systems with directory/file naming/file name extension architectures), as broadly interpreted by the examiner.).

15. Claim 13 ***additionally recites*** the limitation that; "The method of Claim 1, wherein upon a determination that said last file name extension is

not dangerous, said method further comprising:

releasing said file system event.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the scan request servicing (file system event(s), with the

file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware does not exist, unimpeded processing continues), as broadly interpreted by the examiner.).

16. Claim 25 ***additionally recites*** the limitation that; "The system of Claim 24, wherein said anti-viral application is

a behavior blocking application.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the anti-viral application scan request servicing (file system event(s), with the file name extension parsing as a filtering parameter for the malware detection/processing, so as upon the malware processing so determining that malware exists, notification/isolation (i.e., behavior blocking protective actions)/annunciation processing is performed), as broadly interpreted by the examiner.).

17. Claim 28 ***additionally recites*** the limitation that; "The system of Claim 24, wherein said anti-viral application further comprises:

an executable file name extension list;

a file name extension registry; and

an exclusion list.".

The teachings of Muttik et al suggest such limitations (ABSTRACT, figures 1-9 and associated descriptions, para. 0001-0019, whereas the anti-viral application scan request servicing (file system event(s), inclusive of Windows (i.e., the registry inherently encompasses the file types

that include executable file types)/Unix, etc., type file systems with directory/file naming/file name extension architectures), as broadly interpreted by the examiner.).

Allowable Subject Matter

18. Claims 30-33 are allowed over prior art.

19. Claims 11, 12, 14-23, 27 and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

20. Claim 11 ***additionally recites*** the limitation that; "The method of Claim 1, wherein said parsing said file name further obtains

at least a next to last file name extension of said file name.".

21. Claim 12 ***additionally recites*** the limitation that; "The method of Claim 1, wherein upon a determination, that said last file name extension is

the only file name extension of said file name, said method further comprising:

releasing said file system event.".

22. Claim 14 ***additionally recites*** the limitation that; "The method of Claim 1, further comprising:

prior to said determining whether said last file name extension is a dangerous file name extension,

determining whether a by-pass option is selected,

wherein selection of said by-pass option by-passes

said determining whether said last file name extension is

a dangerous file name extension when

said last file name extension is

visible to a user; and

upon a determination that said by-pass option is selected,

determining whether said last file name extension is

visible to a user.".

23. Claim 15 ***additionally recites*** the limitation that; "The method of Claim 14, wherein upon a determination that said last file name extension is not visible to a user,

said method further comprising:

performing said determining whether

said last file name extension is

a dangerous file name extension.".

24. Claim 16 ***additionally recites*** the limitation that; "The method of Claim 14, wherein upon a determination that said last file name extension is visible to a user,

said method further comprising:

not performing said determining whether

said last file name extension is

a dangerous file name extension; and

releasing said file system event.".

25. Claim 17 ***additionally recites*** the limitation that; "The method of Claim 14, wherein upon a determination that said by-pass option is not selected,

said method further comprising:

performing said determining whether

said last file name extension is

a dangerous file name extension.".

26. Claim 18 ***additionally recites*** the limitation that; "The method of Claim 11, wherein said determining whether said last file name extension is

a dangerous file name extension comprises:

determining said last file name extension;

determining whether said last file name extension is

an executable file name extension;

upon a determination that said last file name extension is

an executable file name extension,

determining said next to last file name extension;

determining whether said next to last file name extension is

a registered file name extension;

upon a determination that said next to last file name extension is

a registered file name extension,

determining whether said next to last file name extension is

an excluded file name extension; and

upon a determination that said next to last file name extension is

not an excluded file name extension,

determining that said last file name extension is

dangerous.".

27. Claim 19 ***additionally recites*** the limitation that; "The method of Claim 18, wherein upon a determination that said last file name extension

is not an executable file name extension, said method further comprising:

releasing said file system event.".

28. Claim 20 ***additionally recites*** the limitation that; "The method of Claim 18, wherein said determining whether said last file name extension is an executable file name extension, comprises:

comparing

said last file name extension to

one or more entries of executable file name extensions in

an executable file name extension list

to determine whether

said last file name extension matches

at least one of said one or more entries of

executable file name extensions;

upon a determination that said last file name extension matches

said at least one of said one or more entries of

executable file name extensions,

determining said last file name extension is

an executable file name extension; and

upon a determination that said last file name extension does not match

said at least one of said one or more entries of

executable file name extension,

determining said last file name extension is

not an executable file name extension.".

29. Claim 21 ***additionally recites*** the limitation that; "The method of Claim 18, wherein said determining whether said last file name extension is an executable file name extension, comprises:

locating a file associated with said file name;

opening said file to access the contents of said file;

examining said contents to

determine whether said file is an executable file;

wherein upon a determination that said file is an executable file,

determining said last file name extension is

an executable file name extension; and

wherein upon a determination that said file is not an executable file,

determining said that said last file name extension is

not an executable file name extension.".

30. Claim 22 ***additionally recites*** the limitation that; "The method of Claim 18, wherein upon a determination that said next to last file name extension is

not a registered file name extension,

said method further comprising:

determining that said last file name extension is

not dangerous.".

31. Claim 23 ***additionally recites*** the limitation that; "The method of Claim 18, wherein upon a determination that said next to last file name extension is

an excluded file name extension,

said method further comprising:

determining that said last file name extension is

not dangerous.".

32. Claim 27 ***additionally recites*** the limitation that; "The system of Claim 24, wherein

said detection application comprises:

a parsing module

for obtaining said file name and

for parsing said file name to obtain at least

a last file name extension, and

a next to last file name extension, when present, of said file name;

a logic module

for determining whether said last file name extension is

a dangerous file name extension; and

a found file name extension(s) list

for storing at least

said last file name extension and

said next to last file name extension, when present.".

33. Claim 29 ***additionally recites*** the limitation that; "The system of Claim 27, wherein said detection application further comprises:

an executable file name extension list;

a file name extension registry; and

an exclusion list.".

34. As per claim 30; "A computer program product comprising a computer-readable medium containing computer program code for a method comprising:

stalling a file system event,

said file system event including a file name;

parsing said file name to obtain at least

a last file name extension, and

a next to last file name extension, when present, of said file name;

determining whether said last file name extension is

the only file name extension of said file name;

upon a determination that said last file name extension is

not the only file name extension of said file name,

determining whether said last file name extension is

a dangerous file name extension; and

upon a determination that said last file name extension is

a dangerous file name extension,

generating a notification.".

35. Claim 31 ***additionally recites*** the limitation that; "The computer program product of Claim 30, said method further comprising:

implementing protective actions.".

36. Claim 32 ***additionally recites*** the limitation that; "The computer program product of claim 30, said method further comprising:

terminating said file system event.".

37. Claim 33 ***additionally recites*** the limitation that; "The computer program product of Claim 30, wherein said determining whether said last file name extension is a dangerous file name extension comprises:

determining said last file name extension;

determining whether said last file name extension is an executable file name extension;

upon a determination that said last file name extension is an executable file name extension, determining said next to last file name extension;

determining whether said next to last file name extension is a registered file name extension;

upon a determination that said next to last file name extension is a registered file name extension, determining whether said next to last file name extension is an excluded file name extension; and

upon a determination that said next to last file name extension is not an excluded file name extension, determining that said last file name extension is dangerous.".

Conclusion

38. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6/13/07